80

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/915,511	07/26/2001	Michael Wayne Brown	AUS920010528US1	6703

43307 7590 07/25/2005

IBM CORP (AP)
C/O AMY PATTILLO
P. O. BOX 161327
AUSTIN, TX 78716

EXAMINER	
WILLIAMS, JEFFERY L	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 07/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/915,511	**Applicant(s)** BROWN ET AL.	
	Examiner Jeffery Williams	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _25 April 2005_.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-38_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-38_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _28 September 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _2/07/05_.

4) ☒ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 4/25/2005.

All rejections not set forth below have been withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 – 5, 7 – 9, 11 – 13, 15 – 17, 19 – 21, 23 – 25, and 27 - 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeSimone et al., US Patent: 6,212,548 B1 in view of Smithies et al., US Patent: 6,091,835.

Regarding claim 1, DeSimone et al. discloses a method for enabling a messaging session comprising a plurality of users participating in the session. The participating users are able to view the history of the messaging session in the form of a 'conversation', a string of recorded messages (Col. 2, lines 48-56; Col. 3, lines 43-53). DeSimone et al. does not disclose that the messaging session is verifiable by attaching digital signatures of the participants to the recording of the session. DeSimone et al., however, does teach the understanding that certain messaging sessions between users may need measures of security provided (Col. 14, lines 50-54).

Smithies et al. discloses a method for recording a verifiable transcript of statements, transactions, or events between parties by attaching digital signatures of the participants to the transcript (Col. 3, lines 40-61; Col. 41, lines 21-36).

To combine the method for enabling a messaging session and a history of the session between participants with a method for recoding digital signatures of participants along with the transcript would provide a needed measure of security. Therefore, it would have been obvious to one ordinarily skilled in the art to combine the method of DeSimone et al. with the method of Smithies et al., because it is obvious that certain messaging sessions between users will require the level of verifiability and accountability that a digitally signed transcript would provide.

Regarding claim 2, the combination of DeSimone et al. and Smithies et al. discloses the recording of the selection of message entries and attaching the plurality of digital signatures at a messaging server system connected via a network to a plurality of client systems accessible to the plurality of users (Smithies et al., Fig. 2, Col. 3, lines 40-61; Col. 9, lines 56-63; Col. 41, lines 21-36). As shown by Smithies et al., the transcript generator module may reside on a system other than a client system that has access to it. In this case, digital signatures from a plurality of interacting client systems will be attached at the messaging server system.

Regarding claim 3, the combination of DeSimone et al. and Smithies et al. discloses the recording of the selection of message entries and attaching the plurality of digital signatures at a client system connected via a network to a plurality of client systems accessible to the plurality of users (Smithies et al., Fig. 1, Col. 3, lines 40-61; Col. 8, lines 15-40; Col. 41, lines 21-36). As shown by Smithies et al., when the client application and the transcript generator module both reside on the client system, then the digital signatures will be attached at the client system.

Regarding claim 4, the combination of DeSimone et al. and Smithies et al. discloses a method for verifying a messaging session, wherein verifying includes at least one of verifying at least one of a plurality of digital signatures and verifying an integrity of the messaging session (Smithies et al., Col. 9, line 64 – Col. 10, line 9; Col. 11, lines 44-67). As disclosed by Smithies et al., the transcript generator module will perform session verification functions upon the transcript, such as verification of signatures and verification of the transcript checksum.

Regarding claim 5, the combination of DeSimone et al. and Smithies et al. discloses a method for transmitting a request to a plurality of users to each attach a digital signature to a recording of a selection of message entries from a messaging session. (Smithies et al., Col. 41, lines 21-36, Col. 44, lines 46-56). As disclosed by Smithies et al., multiple parties, or users, can engage in the generation of a transcript.

The transcript generator module will request participants to the session to provide their digital signatures to the transcript.

Regarding claim 7, the combination of DeSimone et al. and Smithies et al. discloses a method for calculating a checksum for the recording of the selection of message entries from the messaging session; and encrypting the checksum utilizing a private key for a particular digital signature from among the plurality of digital signatures, wherein a particular public key is enabled to decrypt the encrypted checksum (Smithies et al., Col. 8, lines 24-43; Col. 14, lines 26-39).

Regarding claim 8, the combination of DeSimone et al. and Smithies et al. discloses a method for verifying an integrity of a selection of message entries by calculating a current checksum for the selection of the plurality of message entries; decrypting said encrypted checksum with a particular public key; and comparing the current checksum with the decrypted checksum, wherein the integrity is verified if the decrypted checksum matches the current checksum (Smithies et al., Col. 14, lines 26-39).

Regarding claim 9, the combination of DeSimone et al. and Smithies et al. discloses a method for verifying a particular digital signature from among a plurality of digital signatures in order to verify a particular user from among a plurality of users associated with the particular digital signature (Smithies et al., Col. 41, lines 7-13, 21-36).

Regarding claim 11, DeSimone et al. discloses a system for recording a message session comprising a server system communicatively connected to a network (Col. 3, line 43 – Col. 4, line 18). DeSimone et al. does not disclose the server system comprising means to record the selection of message entries and means for attaching the digital signatures of the session participants to the recording of the selection of message entries.

Smithies et al. discloses means to record a transcript (the selection of message entries from the plurality of users) as well as a means for attaching the digital signatures of the session participants to the recording of the selection of message entries (Col. 7, lines 41-50; Col. 24, lines 48-55; Col. 41, lines 24-35; Col. 41, line 64 - Col. 42, line 37). As disclosed by Smithies et al., communicating parties can digitally sign a transcript, generated by a transcript generator module that is residing on a server.

The combination of the methods of DeSimone et al. and Smithies et al., as explained regarding claim 1, would obviously be utilized in a system. Thus, it would have been obvious to one ordinarily skilled in the art to combine the system of DeSimone et al. with the system of Smithies et al., because it is obvious that certain systems that record messaging sessions between users will require the level of verifiability and accountability that a system utilizing a digitally signed transcript would provide.

Regarding claim 12, the combination of DeSimone et al. and Smithies et al. discloses a logging controller for verifying a messaging session, wherein the verifying includes at least one of verifying at least one of a plurality of digital signatures and verifying an integrity of the messaging session (Smithies et al., Col. 9, line 64 – Col. 10, line 9; Col. 11, lines 44-67). As disclosed by Smithies et al., the transcript generator module will perform session verification functions upon the transcript, such as verification of signatures and verification of the transcript checksum.

Regarding claim 13, the combination of DeSimone et al. and Smithies et al. discloses a system means for transmitting a request to a plurality of users to each attach a digital signature to a recording of a selection of message entries from a messaging session. (Smithies et al., Col. 41, lines 21-36, Col. 44, lines 46-56). In the system, as disclosed by Smithies, multiple parties, or users, can engage in the generation of a transcript. The transcript generator module will request participants to the session to provide their digital signatures to the transcript.

Regarding claim 15, the combination of DeSimone et al. and Smithies et al. discloses a system means for calculating a checksum for the recording of a selection of message entries from a messaging session; and means for encrypting a checksum utilizing a private key for a particular digital signature from among a plurality of digital signatures, wherein a particular public key is enabled to decrypt the encrypted checksum (Smithies et al., Col. 8, lines 24-43; Col. 14, lines 26-39).

Regarding claim 16, the combination of DeSimone et al. and Smithies et al. discloses a system means for verifying an integrity of a selection of a plurality of message entries by calculating a current checksum for the selection of the plurality of message entries; decrypting said encrypted checksum with a particular public key; and comparing the current checksum with the decrypted checksum, wherein the integrity is verified if the decrypted checksum matches the current checksum (Smithies et al., Col. 14, lines 26-39).

Regarding claim 17, the combination of DeSimone et al. and Smithies et al. discloses a system means for verifying a particular digital signature from among a plurality of digital signatures in order to verify a particular user from among a plurality of users associated with the particular digital signature (Smithies et al., Col. 41, lines 7-13, 21-36).

Regarding claim 19, DeSimone et al. discloses both a method and system implementing the method for recording a message session, as explained in claims 1 and 11. DeSimone et al. does not directly disclose the system utilizing a method that has been implemented in a program residing on a computer readable medium.

Smithies et al. discloses a program means for enabling a recording of a transcript (the selection of message entries from the plurality of users) as well as a program means for attaching the digital signatures of the session participants to the recording of the selection of message entries (Col. 7, lines 41-50; Col. 24, lines 48-55; Col. 41, lines 24-35; Col. 41, line 64 - Col. 42, line 37). As disclosed by Smithies et al., communicating parties can digitally sign a transcript by running browser software enhanced by Java code downloaded from a server.

The combination of the methods/systems of DeSimone et al. and Smithies et al., as explained regarding claims 1 and 11, would obviously incorporate a program means and a computer readable medium embodied by the program means. Thus, it would have been obvious to one ordinarily skilled in the art to combine the system/method means of DeSimone et al. with the system/method/program means of Smithies et al., because it is obvious that systems utilizing methods for recording messaging sessions between users will require program means for practical implementation.

Regarding claim 20, the combination of DeSimone et al. and Smithies et al. discloses program means for enabling verification of a messaging session, wherein verifying includes at least one of verifying at least one of a plurality of digital signatures and verifying an integrity of the messaging session. (Smithies et al., Col. 9, line 64 – Col. 10, line 9; Col. 11, lines 44-67). As disclosed by Smithies et al., the transcript generator module will perform session verification functions upon the transcript, such as verification of signatures and verification of the transcript checksum. Further, as disclosed by Smithies et al., with reference to claim 19, the transcript generator module and other supporting system components are implemented as programs.

Regarding claim 21, the combination of DeSimone et al. and Smithies et al. discloses a program means for controlling transmission of a request to a plurality of users to each attach a digital signature to a recording of said selection of message entries from a messaging session. (Smithies et al., Col. 41, lines 21-36, Col. 44, lines 46-56). In the program means, as disclosed by Smithies et al., multiple parties, or users, can engage in the generation of a transcript. The transcript generator module will request participants to the session to provide their digital signatures to the transcript.

Regarding claim 23, the combination of DeSimone et al. and Smithies et al. discloses a program means for calculating a checksum for a recording of a selection of message entries from a messaging session; and means for enabling encryption of the checksum utilizing a private key for a particular digital signature from among a plurality of digital signatures, wherein a particular public key enabled to decrypt the encrypted checksum (Smithies et al., Col. 8, lines 24-43; Col. 14, lines 26-39).

Regarding claim 24, the combination of DeSimone et al. and Smithies et al. discloses a program means for verifying an integrity of a selection of a plurality of message entries by calculating a current checksum for the selection of the plurality of message entries; decrypting said encrypted checksum with a particular public key; and comparing the current checksum with the decrypted checksum, wherein the integrity is verified if the decrypted checksum matches the current checksum (Smithies et al., Col. 14, lines 26-39).

Regarding claim 25, the combination of DeSimone et al. and Smithies et al. discloses a program means for verifying a particular digital signature from among a plurality of digital signatures in order to verify a particular user from among a plurality of users associated with the particular digital signature (Smithies et al., Col. 41, lines 7-13, 21-36).

Regarding claim 27, the combination of DeSimone et al. and Smithies et al. discloses a method for attaching a digital signature for a sender of a message entry to the message entry; and distributing the message entry to a plurality of participants in a messaging session, wherein each of the plurality of participants in the messaging session are enabled to verify the message entry with the digital signature in real-time (Smithies et al., Col. 13, lines 14-51; Col. 12, lines 14-16, 51-54; Col. 14, line 65 – Col. 15, line 4; Col. 41, lines 24-36). As disclosed by Smithies et al., messages created by an individual through a client application are 'affirmed' (i.e. digitally signed) by the individual. They are then added to the transcript, where other participants through their respective client applications can view the transcript of messages, verify signatures of the messages, and add their own messages.

Regarding claim 28, the combination of DeSimone et al. and Smithies et al. discloses a method for attaching a digital signature for a sender at a client messaging system before distribution within a network (Smithies et al., Fig. 1, Col. 8, lines 15-40; Col. 41, lines 21-36). As shown by Smithies et al., when the client application and the transcript generator module both reside on the client system, then the digital signatures will be attached at the client system.

Regarding claim 29, the combination of DeSimone et al. and Smithies et al. discloses a method for attaching a digital signature for a sender at a messaging server before distribution to a plurality of participants (Smithies et al., Fig. 2, Col. 3, lines 40-61; Col. 9, lines 56-63; Col. 41, lines 21-36). As shown by Smithies et al., the transcript generator module may reside on a system other than a client system that has access to it. In this case, digital signatures from a plurality of interacting client systems will be attached at the messaging server system.

Regarding claim 30, the combination of DeSimone et al. and Smithies et al. discloses a method for verifying at least one of an identity of a sender and an integrity of content of said message entry (Smithies et al., Col. 9, line 64 – Col. 10, line 9; Col. 11, lines 44-67; Col. 13, lines 14-45; Col. 14, line 65 – Col. 15, line 4). As disclosed by Smithies et al., a user via a client application can utilize the transcript generator module to perform session verification functions upon the transcript, such as verification of statements ('message entries') and their corresponding signatures.

Regarding claim 31, the combination of DeSimone et al. and Smithies et al. discloses a messaging system means for attaching a digital signature for a sender of a message entry to the message entry; and means for distributing the message entry to a plurality of participants in a messaging session, wherein each of the plurality of participants in the messaging session are enabled to verify the message entry with the digital signature in real-time (Smithies et al., Col. 13, lines 14-51; Col. 12, lines 14-16, 51-54; Col. 14, line 65 – Col. 15, line 4; Col. 41, lines 24-36). As disclosed by Smithies et al., messages created by an individual through a client application are 'affirmed' (i.e. digitally signed) by the individual. They are then added to the transcript, where other participants through their respective client applications can view the transcript of messages, verify signatures of the messages, and add their own messages.

Regarding claim 32, the combination of DeSimone et al. and Smithies et al. discloses a system means for attaching a digital signature for a sender at a client messaging system before distribution within a network (Smithies et al., Fig. 1, Col. 8, lines 15-40; Col. 41, lines 21-36). As shown by Smithies et al., when the client application and the transcript generator module both reside on the client system, then the digital signatures will be attached at the client system.

Regarding claim 33, the combination of DeSimone et al. and Smithies et al. discloses a system means for attaching a digital signature for a sender at a messaging server before distribution to a plurality of participants (Smithies et al., Fig. 2, Col. 3, lines 40-61; Col. 9, lines 56-63; Col. 41, lines 21-36). As shown by Smithies et al., the transcript generator module may reside on a system other than a client system that has access to it. In this case, digital signatures from a plurality of interacting client systems will be attached at the messaging server system.

Regarding claim 34, the combination of DeSimone et al. and Smithies et al. discloses a system means for verifying at least one of an identity of a sender and an integrity of content of said message entry (Smithies et al., Col. 9, line 64 – Col. 10, line 9; Col. 11, lines 44-67; Col. 13, lines 14-45; Col. 14, line 65 – Col. 15, line 4). As disclosed by Smithies et al., a user via a client application can utilize the transcript generator module to perform session verification functions upon the transcript, such as verification of statements ('message entries') and their corresponding signatures.

Regarding claim 35, the combination of DeSimone et al. and Smithies et al. discloses a program means for enabling attachment of a digital signature for a sender of a message entry to the message entry; and means for controlling distribution of the message entry to a plurality of participants in a messaging session, wherein each of the plurality of participants in the messaging session are enabled to verify the message entry with the digital signature in real-time (Smithies et al., Col. 13, lines 14-51; Col. 12, lines 14-16, 51-54; Col. 14, line 65 – Col. 15, line 4; Col. 41, lines 24-36). As disclosed by Smithies et al., messages created by an individual through a client application are 'affirmed' (i.e. digitally signed) by the individual. They are then added to the transcript, where other participants through their respective client applications can view the transcript of messages, verify signatures of the messages, and add their own messages.

Regarding claim 36, the combination of DeSimone et al. and Smithies et al. discloses a program means for enabling attachment of a digital signature for a sender at a client messaging system before distribution within a network (Smithies et al., Fig. 1, Col. 8, lines 15-40; Col. 41, lines 21-36). As shown by Smithies et al., when the client application and the transcript generator module both reside on the client system, then the digital signatures will be attached at the client system.

Regarding claim 37, the combination of DeSimone et al. and Smithies et al. discloses a program means for enabling attachment of a digital signature for a sender at a messaging server before distribution to a plurality of participants (Smithies et al., Fig. 2, Col. 3, lines 40-61; Col. 9, lines 56-63; Col. 41, lines 21-36). As shown by Smithies et'al., the transcript generator module may reside on a system other than a client system that has access to it. In this case, digital signatures from a plurality of interacting client systems will be attached at the messaging server system.

Regarding claim 38, the combination of DeSimone et al. and Smithies et al. discloses a program means for verifying at least one of an identity of a sender and an integrity of content of said message entry (Smithies et al., Col. 9, line 64 – Col. 10, line 9; Col. 11, lines 44-67; Col. 13, lines 14-45; Col. 14, line 65 – Col. 15, line 4). As disclosed by Smithies et al., a user via a client application can utilize the transcript generator module to perform session verification functions upon the transcript, such as verification of statements ('message entries') and their corresponding signatures.

Claims 6, 10, 14, 18, 22, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeSimone et al. in view of Smithies et al., as applied to claims 1, 9, 11, 17, 19, and 25 above, and further in view of Schneier, Applied Cryptography.

Regarding claim 6, the combination of DeSimone et al. and Smithies et al. discloses a method, system, and program for recording a verifiable messaging session. The messaging session comprises a plurality of users participating in the session. The participating users are able to view the history of the messaging session in the form of a 'conversation', a string of recorded messages (DeSimone et al., Col. 2, lines 48-56; Col. 3, lines 43-53). They disclose the recording of a verifiable transcript of statements, transactions, or events.between parties by attaching digital signatures of the participants to the transcript (Smithies et al., Col. 3, lines 40-61; Col. 41, lines 21-36). Further more, they disclose a signature verification system for the verification of digital signatures that are associated with a plurality of users who participate in the generation of a messaging session (Smithies et al., Col. 9, line 64 – Col. 10, line 9; Col. 11, lines

44-67). The combination of DeSimone et al. and Smithies et al., however, does not disclose the storing of the plurality of keys used by the signature verification system for verifying the plurality of digital signatures belonging to the plurality of users.

Schneier discloses an authentication system using public-key cryptography wherein a plurality of keys are stored for the verification of a plurality of digital signatures belonging to a plurality of users (Pages 53 - 54). As disclosed by Schneier, with public key cryptography, a host safely stores a plurality of keys that are used for authentication ('verification') functions. Such keys must be safely stored so that they may be used later for verification purposes.

It is obvious that any system utilizing public key cryptography to verify the digital signatures of a plurality of users requires a system to manage the usage and storage of such keys. Therefore, it would have been obvious to one ordinarily skilled in the art to combine the method/system/program combination of DeSimone et al. and Smithies et al. with the authentication/verification system of Schneier, because a method/system/program that uses a plurality of public keys for verification requires a system that manages and stores said keys.

Regarding claim 10, in view of the reasons given regarding claim 6, the combination of DeSimone et al., Smithies et al., and Schneier discloses a method for determining whether a public key received order to verify a particular digital signature matches a public key coupled the particular digital signature; and in response to determining a match, verifying a particular user associated with the particular digital signature (Schneier, Page 54, steps 1 – 4). In step 3 of the authentication system, Schneier discloses the looking up of a particular public key coupled to a particular user, and then using that key to decrypt a message. Thus, a determination has been made to use the matching public key that is coupled to a user. In step 4, after performing a successful decryption, the identity of the user is verified.

Regarding claim 14, in view of the reasons given regarding claim 6, the combination of DeSimone et al., Smithies et al., and Schneier discloses a log file repository for storing a plurality of public keys each associated with one from among a plurality of digital signatures such that the plurality of public keys are accessible to a plurality of users for verifying a messaging session (Schneier, Page 53).

Regarding claim 18, in view of the reasons given regarding claim 6, the combination of DeSimone et al., Smithies et al., and Schneier discloses a system means for determining whether a public key received order to verify a particular digital signature matches a public key coupled the particular digital signature; and means for verifying a particular user associated with the particular digital signature, in response to determining a match (Schneier, Page 54, steps 1 – 4). In step 3 of the authentication system, Schneier discloses the looking up of a particular public key coupled to a particular user, and then using that key to decrypt a message. Thus, a determination has been made to use the matching public key that is coupled to a user. In step 4, after performing a successful decryption, the identity of the user is verified.

Regarding claim 22, in view of the reasons given regarding claim 6, the combination of DeSimone et al., Smithies et al., and Schneier discloses a program means for enabling storage of a plurality of keys each associated with one from among a plurality of digital signatures such that the plurality of public keys are accessible to a plurality of users for verifying a messaging session (Schneier, Page 53).

Regarding claim 26, in view of the reasons given regarding claim 6, the combination of DeSimone et al., Smithies et al., and Schneier discloses a program means for determining whether a public key received order to verify a particular digital signature matches a public key coupled the particular digital signature; and means for verifying a particular user associated with the particular digital signature, in response to determining a match (Schneier, Page 54, steps 1 – 4). In step 3 of the authentication system, Schneier discloses the looking up of a particular public key coupled to a particular user, and then using that key to decrypt a message. Thus, a determination has been made to use the matching public key that is coupled to a user. In step 4, after performing a successful decryption, the identity of the user is verified.

Response to Arguments

Applicant's arguments filed 4/25/2005 have been fully considered but they are not persuasive. Applicant argues primarily that:

i. "Claims 1-5, 7-9, 11-13, 15-17, 19-21, 23-25, and 27-38 are not obvious under the combination of DeSimone and Smithies" for the following reasons:

a. "There is no suggestion or motivation to modify DeSimone by Smithies", and "absent such a showing, the Examiner has impermissibly used hindsight occasioned by Applicants' own teaching to reject the claims" (Applicant's Remarks, pages 17, 18).

b. "First, there is not a suggestion or motivation to modify DeSimone in view of Smithies because when DeSimone is viewed as a whole, DeSimone only suggests that policies control which users can be added as new participants to a conversation, and not that "messaging session between users may need measures of security provided" " (Applicant's Remarks, page 19).

c. "Second, there is not a suggestion or motivation to modify DeSimone in view of Smithies because even if DeSimone teaches "the understanding that certain messaging sessions between users may need measures of security provided" as asserted by the Examiner, DeSimone only teaches applying security to limit those users who can add to a conversation, which does not suggest or motivate modifying DeSimone to teach attaching digital signatures to a recording of a messaging session so that the participants in the messaging session are verifiable." (Applicant's Remarks, page 20).

d. "There is no reasonable expectation of success in the proposed modification of DeSimone by Smithies" (Applicant's Remarks, page 21).

e. "Because prima facie obviousness is not established for claims 1, 11, and 19, at least by virtue of their dependency on claims 1, 11, and 19, dependent claims 2-5, 7-9, 12-13, 15-1 7, 20-21, and 23-25are not obvious in view of DeSimone and Smithies, alone or in combination, under 35 U.S.C. 103(a)" (Applicant's Remarks, page 21).

f. "Applicants note that the Examiner cites the combination of DeSimone and Smithies as disclosing the elements of claim 27, but the Examiner does not point to any specific teaching in DeSimone as grounds for the rejection. Applicants traverse the grounds of rejection in view of the references to Smithies cited by the Examiner. In addition, as to the combination of DeSimone and Smithies, Applicants respectfully assert the arguments made with reference to claim 1, as to the lack of motivation or suggestion for the combination of DeSimone and Smithies and the lack of reasonable expectation of success in the proposed modification, also apply to claims 27, 31, and 35, as a result prima facie obviousness is not proved for claims 27, 31, and 35 and Applications respectfully request allowance of these claims" (Applicant's Remarks, pages 21, 22).

g. "Neither DeSimone nor Smithies, separately or in combination, teaches or suggests all the limitations of claims 27, 31, and 35" because "Smithies does not teach that "messages created by an individual through a client application are 'affirmed' (i.e. digitally signed) by the individual. They are then added to the transcript, where other participants through their respective client applications can view the transcript of messages, verify signatures of the messages, and add their own messages." [Office Action, pp. 11-12]" (Applicant's Remarks, pages 23).

h. "In addition, because prima facie obviousness is not established for claims 27, 31, and 35, at least by virtue of their dependency on claims 27, 31, and 35, dependent claims 28-30, 32-34 and 36-38 are not obvious in view of DeSimone and Smithies, alone or in combination, under 35 U.S.C. §103(a). Because a prima facie case of obviousness is not established for claims 28-30, 32-34, and 36-38, Applicants respectfully request allowance of claims 28-30, 32-34, and 36-38" (Applicant's Remarks, page 25).

ii. Claims 6, 10, 14, 18, 22, and 26 are not obvious under the combination of DeSimone, Smithies, and Scheider" (Applicant's Remarks, page 25) for the following reason:

a. "Claims 6, 10, 14, 18, 22, and 26 stand rejected under 35 U.S.C. §103(a) as being unpatentable over DeSimone in view of Smithies as applied to claims 1, 9, 11, 17, 19, and 25 above, and further in view of

> Schneider, Applied Cryptography. [Office Action. p. 16] Application respectfully assert that because prima facie obviousness is not established for claims 1, 11, and 19 under the combination of DeSimone and Smithies, at least by virtue of their dependency on claims 1, 11, and 19, claims 6, 10, 14, 18, 22, and 26 are not obvious under the combination of DeSimone and Smithies and Applied Cryptography under 35 U.S.C. §103(a). Because a prima facie case of obviousness is not established for claims 6, 10, 14. 18, 22, and 26, Applicants respectfully request allowance of claims 6, 10, 14, 18, 22, and 26.

In response to applicant's argument i(a) that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, DeSimone et al. presents a system for participating and transcribing a messaging session. Particularly, DeSimone et al. describes a chat messaging session and a transcript of the messaging session (DeSimone et al., col. 2, lines 53-56). Smithies et al. describes a digitally signed transcript of communications between parties. Smithies et al. teaches that it is advantageous for purposes of security to digitally sign the transcript with the signatures of the parties, providing a level assurance of the integrity of the transcript (Smithies et al., Abstract; col. 3, lines 40-61; col. 8, lines 2-5; col. 13, lines 33-45; col. 14, lines 48-67; col. 15, line 66 – col. 16, line 16; cols. 19,20,21,22). Thus, it would have been obvious to one of ordinary skill in the art to employ the method of Smithies et al. for a digitally signed transcript with the system of a messaging session and transcript by DeSimone et al. This would have been obvious because one of ordinary skill in the art would have been motivated to provide a level of assurance of the integrity of a transcript for the purposes of security.

The examiner points out that a supplemental motive to the above mentioned combination for providing security to a message transcript via verification may also be found in DeSimone et al. itself. As stated, "DeSimone et al., *however*, does teach the understanding that certain messaging sessions between users may need measures of security provided" (italics added, Office Action, page 3). DeSimone et al. recognizes that messaging sessions differ in the nature of the conversations. For example, some messaging sessions recorded in a transcript are of a purely social and considerably relaxed context. Others are not, and they require measures of security to be taken. DeSimone et al.'s teaching regarding the differing nature of messaging sessions that are recorded in a transcript gives evidence that they must at times be handled in ways to provide for the security of the messaging session and, thus, the resulting transcript. Therefore, this motive to provide security to a messaging session and resulting transcript is supplemental to the motivation clearly shown in both the reference of

Smithies et al. and in the knowledge generally available to one of ordinary skill in the art.

The applicant, however, has argued against the reference of DeSimone individually by asserting that the teaching of DeSimone et al. for requirements of security with respect to messaging sessions can only be applied in the context of policies governing the allowance of participants into a messaging session. Therefore, the examiner would like to reiterate that DeSimone has demonstrated that messaging sessions recorded in a transcript differ in nature, from being relaxed and social to ones requiring security measures. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Thus, the applicant's argument i(a) that there is no suggestion to combine the references of DeSimone et al. and Smithies et al. is unpersuasive.

Further, in response to applicant's argument i(a) that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

In response to applicant's arguments i(b) and i(c), they are shown to be unpersuasive for the reasons supplied in the response to applicant's argument i(a).

In response to applicant's argument i(d), that there is no reasonable expectation of success in the proposed modification of DeSimone et al. by Smithies et al., examiner notes that the applicant has based this argument on the preceding arguments of a lack of motivation to combine. Thus, this argument is shown to be unpersuasive for the reasons supplied in the response to applicant's arguments i(a).

Applicant's argument i(e) is based upon the unpersuasive arguments preceding it, and therefore, argument i(e) is shown to be unpersuasive for the reasons supplied in the response to applicant's arguments i(a).

In response to applicant's argument i(f), the examiner points out that the rejection was made upon the grounds of the combination of DeSimone et al. and Smithies et al., as previously stated in the examiner's first office action. Further, the applicant's argument i(f) is based upon the unpersuasive arguments i(a-d), and therefore, argument i(f) is also shown to be unpersuasive for the reasons supplied in the response to applicant's arguments i(a-d).

Regarding the applicant's argument i(g), that neither DeSimone nor Smithies, separately or in combination, teaches or suggests all the limitations of claims 27, 31, and 35, the applicant provides the following reason: "Smithies does not teach, however, the assertions made by the Examiner as to its teaching and its teaching do not teach the elements of claim 27. The Examiner incorrectly asserts that the affirmed document or "message" is added to the transcript, where other participants can view the transcript of messages, verify signatures of the messages, and add their own messages. In particular, Smithies teaches that documents are affirmed by an individual and that the responses during the affirmation process are stored in a transcript object; the document or "message" is not stored in the transcript" (Applicant's Remarks, page 24).

In response to this argument, the examiner points out that the applicant has misinterpreted the examiner's rejection. First, the examiner has not asserted that the affirmed document is the equivalent to the "message". Second, the examiner has not asserted that the affirmed document is stored in the transcript object. Smithies et al. demonstrates a system for allowing a plurality of parties to engage in a messaging session of interactions, such as statements and affirmations, concerning a particular subject such as a transaction, event, or document. The session is recorded in a transcript and associated with digital signatures for the security of the messaging session, allowing the participants to be verified (Smithies et al., Abstract; col. 3, lines 40-61; col. 8, lines 2-5; col. 13, lines 33-45; col. 14, lines 48-67; col. 15, line 66 – col. 16, line 16; cols. 19,20,21,22).

In addition, regarding this argument, the examiner points out that the applicant has mischaracterized the reference of Smithies et al. Namely, the applicant asserts: "Where multiple individuals affirm a document, a separate transcript object is created for each affirmation; individuals do not open an affirmation transcript (transcript object) and add their own documents or "messages" to that transcript object" (Applicant's Remarks, page 24). On the contrary, Smithies discloses that a transcript object is passed between the application clients of the plurality of parties. During the messaging ("affirmation") session, the parties may verify the signatures associated with the transcript that is stored in the transcript object, but they may not change anything previously recorded in the transcript. Thus, while the parties are enabled to make identical copies of the transcript object and the transcript contain therein, the parties may not change the transcript and thereby create a separate or unrelated transcript object. Smithies et al., further discloses that the parties may, in succession, add to the record of the transcript object their own statements or affirmations (Smithies et al., fig. 2; cols. 40, 41).

Finally, regarding this argument, the examiner points out that the rejection of claim 27 was upon the grounds of the combination of DeSimone et al. and Smithies et al. As was shown by the examiner, the combination is specifically the method of recording digital signatures of participants along with a messaging transcript (the participants' signatures being verifiable by viewers of the transcript) as taught by Smithies et al. with the method of DeSimone et al. for enabling a messaging ("chat") session between users and the recording of a transcript (the transcript being viewable in real time by the participants) of the session (Office Action, pages 2, 3).

Thus, the applicant's argument i(g) is shown to be unpersuasive, as the combination of DeSimone et al. and Smithies et al. teaches the limitations of claims 27, 31, and 35.

In response to applicant's arguments i(h), it is shown to be unpersuasive for the reasons supplied in the response to applicant's argument i(g).

In response to applicant's arguments i(h), it is shown to be unpersuasive for the reasons supplied in the response to applicant's argument i(g).

In response to applicant's arguments ii(a), the argument is based solely upon the preceding unpersuasive arguments and it is shown to be unpersuasive for the reasons supplied in the responses above to applicant's arguments i(a-g).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
Assistant Examiner
Art Unit 2137
7.13.2005

Matthew D. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137